ACI UNIVERSAL PAYMENTS℠

3D SECURE – THE BENEFITS OF A RISK-BASED APPROACH TO AUTHENTICATION

The introduction of the 3D Secure (3DS) authentication protocol over 10 years ago was intended to increase the security of online commerce, promote consumer confidence and enable merchants to harness eCommerce growth opportunities. The protocol makes eCommerce safer for merchants, shifting the liability for fraudulent transactions to the issuer, and can enable significant savings on interchange fees. It has, however, had a mixed reception.

In a number of countries, the adoption of 3DS initially resulted in a high level of payment failures, causing losses for merchants and frustration for customers. Anecdotal evidence in the early years suggested that some European retailers suffered up to a 70% drop in online sales following 3DS implementation due largely to forgotten passwords, a lack of understanding and mistrust on the part of consumers.

In most cases, these teething troubles reduce as consumer awareness increases and, today, 3DS has had an overwhelmingly positive impact on conversion rates in countries such as India, Russia and the U.K. In contrast, it is reported as having a negative impact in Brazil, China, France, Germany and the U.S. The extra step that 3DS adds to the checkout process continues to lead some shoppers to abandon their purchases at the last minute in favor of other shopping methods or merchants.

TAKING A RISK-BASED APPROACH

Licensed by Visa and MasterCard, an increasing number of issuers are implementing a risk-based approach to authentication, categorizing transactions as high-, medium- or low-risk and, on the basis of that risk, determining whether the cardholder is required to fully authenticate themselves through 3DS. This both improves the cardholder's customer experience and directly benefits merchants — who can continue sending transactions that do not require 3DS authentication through to the issuer to enjoy the liability shift and interchange benefits.
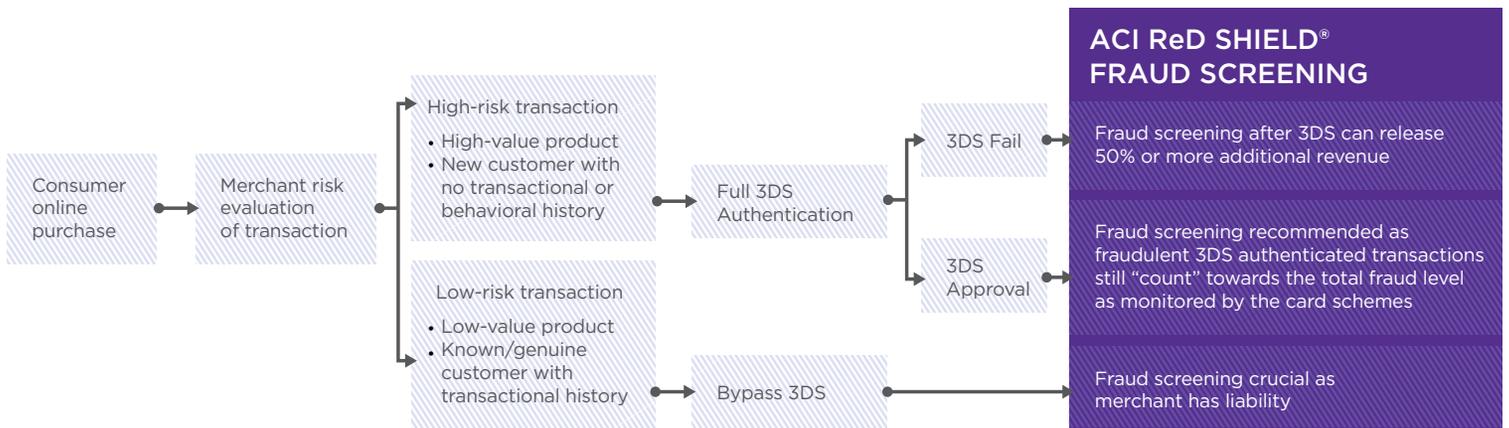
BENEFITS OF RISK-BASED 3DS

- Reduced cart abandonment
- Improved experience for genuine customers
- Faster check-out times
- Can remove need for card enrollment

On average, 40-50% of U.S. transactions are low-risk and likely to be eligible for full fraud liability shift and interchange discount, with no interruption or messaging during checkout and no risk of abandonment.

More merchants are themselves taking a risk-based approach, deciding when to require 3DS authentication and when to accept liability. Using a combination of customer data, behavioral and transactional history, and product information, merchants can create a strategy which allows lower-risk/lower-value transactions and genuine customers to bypass 3DS altogether.

EXAMPLE OF RISK-BASED 3D SECURE AUTHENTICATION PROCESS FLOW

Consumer online purchase → Merchant risk evaluation of transaction →

High-risk transaction
- High-value product
- New customer with no transactional or behavioral history

→ Full 3DS Authentication →
- 3DS Fail
- 3DS Approval

Low-risk transaction
- Low-value product
- Known/genuine customer with transactional history

→ Bypass 3DS

ACI ReD SHIELD® FRAUD SCREENING

Fraud screening after 3DS can release 50% or more additional revenue

Fraud screening recommended as fraudulent 3DS authenticated transactions still "count" towards the total fraud level as monitored by the card schemes

Fraud screening crucial as merchant has liability

BEYOND 3DS

ACI works with merchants around the world to implement flexible and tailored rule strategies with 3DS operating as one element in a holistic, risk-based approach to authentication. Implementing the ACI ReD Shield fraud prevention solution before bank authorization enables merchants to identify loyal customers and low-risk transactions which they may want to approve without applying 3DS. Implementing ACI ReD Shield post-authorization can help establish why a transaction may have failed 3DS. Where appropriate, ACI can then act in real time to retrieve failed 3DS transactions and facilitate any genuine business that has been declined. In some instances ACI has seen 50% or more of failed 3DS transactions converted into additional revenue once rescreened.

Finally, a word of caution. While 3DS provides merchants with protection in terms of liability shift, any fraudulent 3DS authenticated transactions still "count" towards the total fraud level, as monitored by the card schemes. It isn't enough to put 3DS in place and assume that this lifts the threat of scheme fines. What is more, where fraud levels exceed scheme parameters, and the scheme believes improvements have not been made, the liability shift may be invalidated, leaving the merchant to bear the cost of both the fraudulent transactions and the incurred fines.

ATL5573 11-14

ABOUT ACI WORLDWIDE

ACI Worldwide, the Universal Payments company, powers electronic payments and banking for more than 5,000 financial institutions, retailers, billers and processors around the world. ACI software processes $13 trillion each day in payments and securities transactions for more than 250 of the leading global retailers, and 21 of the world's 25 largest banks. Universal Payments — 🆙 — is ACI's strategy to deliver the industry's broadest, most unified end-to-end enterprise payment solutions. Through our comprehensive suite of software products and hosted services, we deliver solutions for payments processing; card and merchant management; online banking; mobile, branch and voice banking; fraud detection; trade finance; and electronic bill presentment and payment. To learn more about ACI, please visit www.aciworldwide.com. You can also find us on Twitter @ACI_Worldwide.